Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A hybrid authentication system for securing digital communications in a network and enabling a global enterprise, comprising:
a distributed authentication infrastructure including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification and intended to perform a series of functions, one of said series of functions for verifying said identification of said plurality of nodes; and
a centralized authentication infrastructure integrated into said distributed authentication infrastructure and including a central server, said central server being coupled to said plurality of nodes and being utilized for verifying said identification of said plurality of nodes;
wherein said distributed authentication infrastructure is initially implemented and said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure;
wherein said distributed authentication infrastructure is selected from the group consisting of a threshold cryptography service model and a web-of-trust service model;

wherein said centralized authentication system is selected from the group consisting of a public key infrastructure and a kerberos service model.
wherein said plurality of nodes include at least one of a personal digital assistant, a digital pager, a digital fax machine, a vide teleconferencing device, a wireless telephone, a portable computer, a desktop computer, and a communication device.

[c2] The hybrid authentication system of claim 1 wherein said plurality of nodes includes a verifying node coupled to a new entity for verifying the identification of said new entity and enrolling said new entity into the hybrid authentication system.

[c3] The hybrid authentication system of claim 2 wherein said new entity provides said verifying node with at least one predetermined credential.

[c4] The hybrid authentication system of claim 2 wherein said verifying node signs a certificate related to said new entity.

[c5] The hybrid authentication system of claim 4 wherein said central server publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been re-

voked.

[c6] The hybrid authentication system of claim 4 wherein a quorum of said plurality of nodes publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked.

[c7] The hybrid authentication system of claim 2 wherein said central server is said new entity.

[c8] The hybrid authentication system of claim 1 wherein said distributed authentication infrastructure requires a quorum of said plurality of nodes for enrolling a new entity into the hybrid authentication system.

[c9] The hybrid authentication system of claim 8 wherein each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature.

[c10] The hybrid authentication system of claim 9 wherein said central server publishes a certificate revocation list, each node of said quorum examining said certificate revocation list for determining whether said certificate has been revoked.

[c11] The hybrid authentication system of claim 8 wherein said

central server is said new entity.

[c12] The hybrid authentication system of claim 1 wherein said central server is coupled to a new entity and is utilized for verifying the identification of said new entity and enrolling said new entity into the hybrid authentication system, said central server producing a log for recording a plurality of failed authentications and a plurality of failed enrollments by said plurality of nodes.

[c13] The hybrid authentication system of claim 1 wherein said central server is coupled to said plurality of nodes for at least one of issuing a global directive thereto and bolstering said plurality of nodes by assisting with at least one of an enrollment task, an authentication task, and a permission granting task.

[c14] The hybrid authentication system of claim 13 wherein said global directive includes at least one of a rekey instruction and a critical trust chain path, said rekey instruction and said critical trust chain path for providing a secured data transfer line.

[c15] The hybrid authentication system of claim 1 wherein said plurality of nodes includes a first node and a second node coupled to said first node, said first node presenting a first certificate to said second node for authenti-

cating said first node.

[c16] The hybrid authentication system of claim 15 wherein said second node examines a certificate revocation list prepared by said central server, said second node examining said certificate revocation list for determining whether said first certificate has been revoked.

[c17] The hybrid authentication system of claim 15 wherein said second node examines a certificate revocation list prepared by a quorum of said plurality of nodes, said second node examining said certificate revocation list for determining whether said first certificate has been revoked.

[c18] The hybrid authentication system of claim 15 wherein said second node is coupled to a trusted third party node from said plurality of nodes, said second node producing an authentication task signed by said first node and sending said authentication task to said trusted third party node, said trusted third party node verifying said identification of said first node.

[c19] The hybrid authentication system of claim 15 wherein said second node presents a second certificate to said first node for authenticating said second node.

[c20] The hybrid authentication system of claim 19 wherein

said first node examines a certificate revocation list prepared by said central server, said first node examining said certificate revocation list for determining whether said second certificate has been revoked.

[c21] The hybrid authentication system of claim 19 wherein said first node examines a certificate revocation list prepared by a quorum of said plurality of nodes, said first node examining said certificate revocation list for determining whether said second certificate has been revoked.

[c22] The hybrid authentication system of claim 18 wherein said first node is coupled to a trusted third party node from said plurality of nodes, said first node producing an authentication task signed by said second node and sending said authentication task to said trusted third party node, said trusted third party node verifying said identification of said first node.

[c23] A hybrid authentication system, comprising:
a distributed authentication infrastructure based on a threshold cryptography service model and including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification and intended to perform a series of functions, one of said series of functions for verifying said identification of

said plurality of nodes; and

a centralized authentication infrastructure based on a public key infrastructure and integrated into said distributed authentication infrastructure, said centralized authentication infrastructure including a certificate authority coupled to said plurality of nodes and utilized for verifying said identification of said plurality of nodes; wherein said distributed authentication infrastructure is initially implemented and said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure.

[c24] A hybrid authentication system, comprising:

a distributed authentication infrastructure based on a web-of-trust service model and including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification and intended to perform a series of functions, one of said series of functions for verifying said identification of said plurality of nodes; and

a centralized authentication infrastructure based on a public key infrastructure and integrated into said distributed authentication infrastructure, said centralized authentication infrastructure including a certificate authority coupled to said plurality of nodes and utilized for verifying said identification of said plurality of nodes;

wherein said distributed authentication infrastructure is initially implemented and said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure.

[c25] The hybrid authentication system recited in claim 24 wherein said plurality of nodes is a plurality of members including a first member and a second member, said certificate authority issuing a first group certificate to said first member that provides said first member with a first permission level, said certificate authority issuing a second group certificate to said second member that provides said second member with a second permission level.

[c26] The hybrid authentication system recited in claim 25 wherein said first group certificate enables said first member to enroll a new entity into the system and provide said new entity with a new permission level equivalent up to said first permission level.

[c27] The hybrid authentication system recited in claim 25 wherein said second group certificate enables said second member to enroll a new entity into the system and provide said new entity with a new permission level equivalent up to said second permission level.

[c28] The hybrid authentication system recited in claim 25 wherein said first permission level is greater than said second permission level.

[c29] A hybrid authentication system, comprising:
a distributed authentication infrastructure including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification and intended to perform a series of functions, one of said series of functions for verifying said identification of said plurality of nodes; and
a centralized authentication infrastructure integrated into said distributed authentication infrastructure, said centralized authentication infrastructure including a certificate authority coupled to said plurality of nodes and utilized for verifying said identification of said plurality of nodes;
wherein said distributed authentication infrastructure is initially implemented and said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure.

[c30] The hybrid authentication system of claim 29 wherein said central server is coupled to said plurality of nodes for at least one of issuing a global directive thereto and supporting said plurality of nodes by assisting with at least one of an enrollment task, an authentication task,

and a permission granting task.

[c31] The hybrid authentication system of claim 30 wherein said global directive includes at least one of a rekey instruction and a critical trust chain path, said rekey instruction and said critical trust chain path for providing a secured data transfer line.

[c32] A method for creating the hybrid authentication system recited in claim 1, comprising:
first coupling a plurality of nodes to each other in a distributed authentication infrastructure;
then migrating said distributed authentication infrastructure to a centralized authentication structure; and
allocating at least one of an enrollment function and an authentication function between said central server and said plurality of nodes.

[c33] The method of claim 32 wherein migrating comprises coupling a central server to said plurality of nodes.

[c34] The method recited in claim 33 further comprising:
coupling said central server to a verifying node of said plurality of nodes;
sending at least one predetermined credential from said central server to said verifying node;
enrolling said central server into the hybrid authentica-

tion system.

[c35] The method recited in claim 33 further comprising:
coupling said central server to a verifying node of said plurality of nodes;
sending a certificate revocation list from said central server to said verifying node;
enrolling said central server into the hybrid authentication system.

[c36] The method recited in claim 32 further comprising:
coupling a new entity to one of said plurality of nodes;
sending at least one predetermined credential from said new entity to said verifying node;
enrolling said new entity into the hybrid authentication system.

[c37] The method recited in claim 32 further comprising:
coupling a new entity to a verifying node of said plurality of nodes;
sending a certificate revocation list from said new entity to said verifying node;
enrolling said new entity into the hybrid authentication system.

[c38] The method recited in claim 32 further comprising:
appointing said central server as a proxy for a quorum of

said plurality of nodes and for fulfilling an enrollment task; and

enrolling said new entity into the hybrid authentication system.